

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re application of :
Takahiro NAGAI et al. :
Serial No. NEW : Attn: Application Branch
Filed March 14, 2001 : Attorney Docket No. 2001-0295A

ENCRYPTED DATA SIGNAL, DATA
STORAGE MEDIUM, DATA SIGNAL
PLAYBACK APPARATUS, AND DATA
SIGNAL RECORDING APPARATUS

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEE FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975.

CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2000-070020, filed March 14, 2000, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Takahiro NAGAI et al.

By:

Nils E. Pedersen
Registration No. 33,145
Attorney for Applicants

NEP/pth
Washington, D.C. 20006
Telephone (202) 721-8200
March 14, 2001

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

1c978 U.S. PTO
09/805147
03/14/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

2000年 3月14日

願 番 号
Application Number:

特願2000-070020

願 人
Applicant(s):

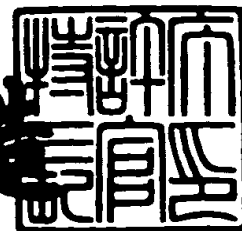
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 1月19日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 2032420119

【提出日】 平成12年 3月14日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 20/10
G09C 5/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 永井 隆弘

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 石原 秀志

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 福島 能久

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 複製世代管理方法、情報信号記録再生方法、情報信号再生装置、情報信号記録装置および情報記録媒体

【特許請求の範囲】

【請求項 1】 複製制御が必要な情報信号を記録する情報記録媒体において、前記情報信号は情報記録媒体上に暗号化状態で記録されることを示す暗号化情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号に暗号化を施した情報信号として記録されることを特徴とする情報記録媒体。

【請求項 2】 前記情報信号は、少なくとも、これ以上の複製禁止、絶対複製禁止の状態である情報信号を記録することを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 3】 前記電子透かし情報は、前記情報信号が暗号化状態で記録されることを示す暗号化情報と、記録される情報記録媒体の種別とを有することを特徴とする請求項 1 または 2 に記載の情報記録媒体。

【請求項 4】 情報記録媒体上に暗号化状態で記録されることを示す暗号化情報が電子透かし情報として重畳された情報信号として記録された情報記録媒体を読み出す情報再生装置において、情報記録媒体から情報を読み出す情報読み出し手段と、前記情報信号が暗号化されているか否かを検出する暗号化状態検出手段と、前記情報信号に電子透かし情報として重畳されている暗号化情報を検出する電子透かし情報検出手段と、前記電子透かし情報と前記暗号化状態検出手段の検出結果を調べ、少なくとも、電子透かし情報の暗号化情報が暗号化状態にあり、暗号化状態検出手段の検出結果が暗号化状態にない場合に、前記情報信号の正常な再生を禁止する再生制御手段と、を備えることを特徴とする情報信号再生装置。

【請求項 5】 請求項 4 に記載の暗号化状態検出手段は、前記情報信号に対して施された暗号化を暗号解読する暗号解読手段として構成され、前記暗号解読手段によって暗号解読動作が行われたか否かによって、暗号化状態を検出することを特徴とする暗号化状態検出手段を備えた情報信号再生装置。

【請求項 6】 請求項 4 に記載の情報信号再生装置において、さらに前記情報

記録媒体の種別を検出する情報記録媒体種別検出手段を有し、前記電子透かし情報として検出された暗号化情報に含まれる情報記録媒体種別と、前記情報記録媒体種別検出手段で検出された前記情報記録媒体の種別とが一致しない場合に前記情報信号の正常な再生を禁止することを特徴とする情報信号再生装置。

【請求項 7】 情報記録媒体上に暗号化状態で記録されることを示す暗号化情報が電子透かし情報として前記情報信号に重畳する電子透かし情報書換手段と、前記電子透かし情報を重畳した情報信号に暗号化を施す暗号化手段と、前記暗号化した情報信号を情報記録媒体に書き込む情報書き込み手段を備えることを特徴とする情報信号記録装置。

【請求項 8】 請求項 7 に記載の情報信号記録装置において、前記暗号化情報は、情報記録媒体上に暗号化されて記録されることを示す暗号化状態と情報記録媒体の種別を電子透かし情報として重畳することを特徴とする前記電子透かし情報書換手段を備えることを特徴とする情報信号記録装置。

【請求項 9】 情報信号に重畳されている電子透かし情報を検出する電子透かし情報検出手段と、前記電子透かし情報として情報信号が暗号化状態で記録されていることを示す暗号化情報が検出された場合に記録を禁止する記録制御手段と、を備えることを特徴とする情報信号記録装置。

【請求項 10】 情報信号再生部と情報信号伸長部とで構成される請求項 4、5 または 6 に記載の情報信号再生装置であって、前記情報信号再生部は、前記情報読み出し手段と、読み出した情報信号をデジタル・インタフェースに送出するデジタル・インタフェース制御手段と、前記情報信号伸長部が正規のものであるか否かを調べる第 1 認証手段を有し、前記情報信号伸長部は、前記暗号解読手段と、前記電子透かし情報検出手段と、前記再生制御手段と、情報信号をデジタル・インタフェースから受信するデジタル・インタフェース制御手段と、前記情報信号再生部が正規のものであるか否かを調べる第 2 認証手段を有し、前記情報信号再生部と前記情報信号伸長部とをデジタル I/F により接続することにより構成されることを特徴とする情報信号再生装置。

【請求項 11】 情報信号記録部と情報信号圧縮部とで構成される請求項 7 または 8 に記載の情報信号記録装置であって、前記情報信号圧縮部は、複製制御情

報検出手段と、前記暗号化手段と、前記電子透かし情報書換手段と、前記記録制御手段と、情報信号をデジタル・インタフェースに送信するデジタル・インタフェース制御手段と、前記情報信号記録部が正規のものであるか否かを調べる第2の認証手段を有し、前記情報信号記録部は、前記情報書き込み手段と、情報信号をデジタル・インタフェースから受信するデジタル・インタフェース制御手段と、前記情報信号圧縮部が正規のものであるか否かを調べる第1の認証手段を有し、前記情報信号圧縮部と前記情報信号記録部とをデジタル・インタフェースにより接続することにより構成されることを特徴とする情報信号記録装置。

【請求項12】 前記第1の認証手段は、情報記録媒体種別判別部において検出した情報記録媒体の種別と認証で使用する共通鍵とから情報記録媒体種別に固有の情報記録媒体認証鍵を生成する演算部を有し、生成した情報記録媒体認証鍵をもとに認証を行うことを特徴とし、前記第2の認証手段は、認証で使用する共通鍵と前記デジタル・インタフェース制御手段で受信した情報記録媒体種別とから固有の情報記録媒体認証鍵を生成する演算部を有し、生成した情報記録媒体認証鍵をもとに認証を行うことを特徴とする、請求項10に記載の情報信号再生装置。

【請求項13】 前記第1の認証手段は、情報記録媒体種別判別部において検出した情報記録媒体の種別と認証で使用する共通鍵とから情報記録媒体種別に固有の情報記録媒体認証鍵を生成する演算部を有し、生成した情報記録媒体認証鍵をもとに認証を行うことを特徴とし、前記第2の認証手段は、認証で使用する共通鍵と前記デジタル・インタフェース制御手段で受信した情報記録媒体種別とから固有の情報記録媒体認証鍵を生成する演算部を有し、生成した情報記録媒体認証鍵をもとに認証を行うことを特徴とする、請求項11に記載の情報信号記録装置。

【請求項14】 前記第2の認証手段であって、さらに情報記録媒体ごとに異なる認証手順、あるいは、情報信号転送手順から情報記録媒体種別を検出することを特徴とする第2認証手段を備える請求項10に記載の情報信号再生装置。

【請求項15】 前記第2の認証手段であって、さらに情報記録媒体ごとに異なる認証手順、あるいは、情報信号転送手順から情報記録媒体種別を検出するこ

とを特徴とする第 2 認証手段を備える請求項 1 1 に記載の情報信号記録装置。

【請求項 1 6】 請求項 1、2 または 3 に記載の情報記録媒体において、さらに、前記情報信号再生部と前記情報信号伸長部、あるいは、前記情報信号圧縮部と前記情報信号記録部の認証に使用する認証鍵ならびに情報記録媒体種別を暗号化した認証鍵情報を有することを特徴とする情報記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタル化された映像や音楽などの著作物の情報信号を情報記録媒体に記録する場合において、情報記録媒体への不正な複製、ならびに、不正に複製された情報記録媒体からの再生を制限する方法、情報記録媒体、ならびに、装置に関する。

【0 0 0 2】

【従来の技術】

近年、デジタルコンテンツの普及により、不正な複製による著作権侵害が大きな問題となっている。これに対し、デジタルコンテンツに複製制御のための情報（複製制御情報）を付加したり、暗号化技術を用いて情報信号を暗号化し、正式にライセンスを受けた機器でないと解読できなくするといった方法により、不正な複製を防止することが考えられる。さらに、複製制御情報を電子透かし情報として、雑音として情報信号に埋め込むことにより、複製制御情報の書換えを防止し、再生制御ならびに記録制御を行うといった方法が提供されている。

【0 0 0 3】

情報信号の複製制御に用いる情報には、“複製可能 (C o p y F r e e)”、“1 回複製可能 (O n e C o p y)”、“これ以上複製禁止 (N o M o r e C o p y)”、“絶対複製禁止 (N e v e r C o p y)” の 4 状態があり、これらによって、情報信号の複製制御状態を表すようにしている。

【0 0 0 4】

以上のような情報を用いて、従来は、複製制御用の付加情報により、画像や音声といった情報信号がもつ複製制御情報をチェックし、“これ以上複製禁止”や

“絶対複製禁止”といった状態の場合は記録を制限することにより、複製世代制限を行っている。しかしながら、複製制御情報をチェックしない記録装置で、“これ以上複製禁止”の状態にある情報信号を記録媒体に記録した場合、1回目の複製により生成されたものと同じものが複製されてしまう。

【0005】

これに対して、特開平11-353796号公報では、情報信号の再生時に情報信号に重畳されている電子透かし情報を書き換えることにより、不正に記録された記録媒体からの再生を実質的に不能とする方法、ならびに装置が提供されている。

【0006】

図13に示すように、情報記録媒体1300に記録された情報信号（電子透かし情報として、“これ以上の複製禁止”を示す情報が重畳）を電子透かし処理に対応した再生装置1301（コンプライアントな再生装置）で再生する際に、情報信号に重畳されている電子透かし情報を“絶対複製禁止”に書き換えて出力する。電子透かし処理に対応した記録装置1302（コンプライアントな記録装置）では、情報信号に重畳されている電子透かし情報を検出し、“絶対複製禁止”の情報信号を記録しないようにすることで、複製に対する制御が行われる。電子透かし処理に対応しない記録装置1303（ノンコンプライアントな記録装置）では、重畳されている電子透かし情報を無視し、記録制限を実施せずに記録媒体1304への情報信号の記録が行われる。しかしながら、不正に記録された記録媒体1304の情報信号には、電子透かし情報として“絶対複製禁止”の情報が重畳されており、電子透かし処理に対応した再生装置1305（コンプライアントな再生装置）では、記録媒体に上記のような“絶対複製禁止”の情報信号が記録されている場合を不正な複製が行われた記録媒体であると判定し、再生を実質的に不能とする。

【0007】

【発明が解決しようとする課題】

以上のようにして、従来は、記録媒体に記録されている情報信号（“これ以上複製禁止”の情報信号）を再生装置で再生する場合、電子透かし情報として重畳

されていた“これ以上複製禁止”の情報を“絶対複製禁止”に書き換え、再生出力信号として送出している。このため、電子透かし情報の書換手段を再生装置にも備えることが不可欠であり、再生装置のコストアップにつながる。

【0008】

本発明は、以上の点に鑑み、不正に作成された記録媒体からの情報信号の再生を実質的に不能にすることにより、有効で安価に複製の防止ができるようにした方法および装置を提供することを目的とする。

【0009】

【課題を解決するための手段】

上記課題を解決するために、本発明の複製世代管理方法は、複製制御が必要な情報信号を記録する情報記録媒体において、少なくとも、これ以上の複製禁止、絶対複製禁止の状態の情報信号である前記情報信号には情報記録媒体上にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号にスクランブルを施した情報信号として記録することを特徴とする。

【0010】

本発明の情報記録再生装置は、これ以上の複製禁止、あるいは、絶対複製禁止の状態である前記情報信号には、情報記録媒体上にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号にスクランブルを施した情報信号として記録された情報記録媒体を読み出す情報再生装置であって、情報記録媒体から情報を読み出す情報読み出し手段と、前記情報信号に対して施されたスクランブルをデスクランブルするデスクランブル手段と、デスクランブルされた情報信号に電子透かし情報として重畳されているスクランブル情報を検出する電子透かし情報検出手段と、前記電子透かし情報とデスクランブル手段のデスクランブル動作を調べ、少なくとも、電子透かし情報のスクランブル情報がスクランブル状態にあり、デスクランブル手段が動作していない場合に、前記情報信号の正常な再生を禁止する再生制御手段とを備える。

【0011】

本発明の情報記録装置は、1回複製可能、これ以上の複製禁止、あるいは、絶対複製禁止の状態の複製制御情報を有する前記情報信号を情報記録媒体に書き込む情報記録装置であって、前記複製制御情報を検出する手段と、検出した複製制御情報が1回複製可能である場合に、情報記録媒体上にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として前記情報信号に重畳する電子透かし情報書換手段と、前記電子透かし情報を重畳した情報信号にスクランブルを施すスクランブル手段と、前記スクランブルした情報信号を情報記録媒体に書き込む情報書き込み手段を備える。

【0012】

本発明の情報信号記録装置は、1回複製可能、これ以上の複製禁止、あるいは、絶対複製禁止の状態の複製制御情報を有する前記情報信号を情報記録媒体に書き込む情報記録装置において、前記複製制御情報を検出する複製制御情報検出手段と、前記情報信号に重畳されている電子透かし情報を検出する電子透かし情報検出手段と、前記電子透かし情報として情報信号がスクランブル状態で記録されていることを示すスクランブル情報が検出された場合に、記録を禁止する記録制御手段とを備える。

【0013】

【発明の実施の形態】

以下、本発明による複製世代管理方法およびこの方法を用いる再生装置、記録装置、情報記録媒体の実施形態について、図を参照しながら説明する。以下に説明する実施の形態は、光ディスクに情報信号を記録する場合であり、複製制御の対象が画像音声情報、光ディスクがDVDの場合である。

【0014】

なお、以下の説明では、記録型のDVDはRAMディスクと称し、また、再生専用のDVDはROMディスクと称することとする。また、複製世代制限処理に対応する記録装置および再生装置をコンプライアントの装置と呼び、複製世代制限処理に対応していない装置をノンコンプライアントの装置と呼ぶ。

【0015】

(実施の形態1)

図 1 は、本発明による複製世代管理方法の実施の形態 1 を説明するための概略図である。この実施の形態 1 においては、ROM ディスク 1 0 0 に映像や音声といった情報信号が記録される。

【 0 0 1 6 】

情報信号が複製制御対象となる場合（例えば、“絶対複製禁止”の情報信号の場合）、正規にライセンスを受けた装置でないと再生できないようにするために、情報信号をスクランブル（暗号化）して記録するものとする。その際、情報信号がスクランブルされた情報であることを示すスクランブル情報“S c r a m b l e d”を、電子透かし情報として情報信号に重畳する。スクランブル処理は電子透かし情報が重畳された情報信号に対し、特定のスクランブル方式（暗号方式）にしたがってスクランブルされた情報信号として ROM ディスク 1 0 0 に記録する。

【 0 0 1 7 】

情報信号が複製制御対象とならない場合（例えば、“複製フリー”の情報の場合）、スクランブルされていないことを示すスクランブル情報“N o n - S c r a m b l e d”が電子透かし情報として重畳された情報信号を ROM ディスクに記録する。あるいは、電子透かし情報を重畳せずに元の情報信号のままを ROM ディスクに記録する。

【 0 0 1 8 】

この結果、複製制御の対象となる ROM ディスクを再生するためには、上記の暗号方式に対するライセンスを受け、復号鍵や復号アルゴリズムに関する情報を取得する必要がある。復号機能を実装したコンプライアントな再生装置 1 0 1 では、ROM ディスク 1 0 0 から情報信号を読み出し、スクランブルが施されている情報信号に対してデスクランブルを行い、出力可能な情報信号を得ることができる。

【 0 0 1 9 】

さらに、デスクランブルされた結果から電子透かし情報を検出し、スクランブルの有無が一致した場合に情報信号の出力を行う。従って、コンプライアントな再生装置の出力信号にはデスクランブルされてはいるが、電子透かし情報として

、“S c r a m b l e d”が重畳された信号が出力される。このように出力された信号は、複製制御対象となり、コンプライアントな記録装置 1 0 2 では“絶対複製禁止”と判断し、R A Mディスクへの記録が禁止される。

【 0 0 2 0 】

また、スクランブルが施されていなかった場合も同様に電子透かし情報を調べ、電子透かし情報が検出されない場合、あるいは電子透かし情報“N o n - S c r a m b l e d”が検出された場合に情報信号の出力を行う。このように出力された信号は、自由に複製が可能であり、コンプライアントな記録装置 1 0 2 での R A Mディスクへの複製が許可される。

【 0 0 2 1 】

図 1 のノンコンプライアントな記録装置 1 0 3 は、複製制御対象である電子透かし情報“S c r a m b l e d”を有する情報信号であるにもかかわらず、電子透かし情報を検出せずに R A Mディスク 1 0 4 への複製を行う。しかしながら、コンプライアントな再生装置 1 0 5 では、電子透かし情報であるスクランブル情報と、情報信号そのものに施されているスクランブルの有無を比較し、比較結果が不一致となる場合は不正に複製した情報信号であると判断し、情報信号の出力を禁止する。

【 0 0 2 2 】

以上のように、図 1 に示したような R O Mディスクにおいて、コンプライアントな再生装置に電子透かし情報の書換手段を実装しなくても、ノンコンプライアントな記録装置によって行われた不正な複製ディスクをコンプライアントな再生装置で再生禁止することができる。

【 0 0 2 3 】

なお、本実施の形態では、電子透かし情報として情報信号に施されているスクランブル情報（“S c r a m b l e d”、“N o n - S c r a m b l e d”）を情報信号に重畳したが、情報信号のスクランブルの状態を示すものであれば他の情報を用いてよい。例えば、R O Mディスクにおいて、複製制御情報である“絶対複製禁止”である情報信号に対して情報信号をスクランブルして記録する場合、この複製制御情報を電子透かし情報として情報信号に重畳しても同様の効果が

得ることができる。

【 0 0 2 4 】

〔記録装置〕

次に、コンプライアントな記録装置 1 0 2 の構成例について図 2 を用いて説明する。図 2 に示すように、このコンプライアントな記録装置は、デジタル入力端子 2 0 1 とアナログ入力端子 2 0 2 を備える。暗号解読部 2 0 3 は、デジタル入力端子に接続される機器から送られてくる暗号鍵情報をもとにデータの暗号化を復号し、圧縮ビデオデータを復元する。この際、入力された情報信号がコピー可能であるかどうかを示すコピー制御情報を検出する。

【 0 0 2 5 】

また、アナログ入力端子を通じて入力されたビデオ情報は、アナログ入力端子 2 0 2 を通じて、エンコード部 2 0 4 に供給されて、M P E G 圧縮され、圧縮ビデオデータが生成される。この際、入力された情報信号がコピー可能であるかどうかを示すコピー制御情報を検出する。

【 0 0 2 6 】

セレクタ 2 0 5 はユーザの入力選択に応じたセレクタ制御信号により、暗号解読部 2 0 3 からのデータと、エンコード部 2 0 4 からのデータとのいずれかを選択して出力する。

【 0 0 2 7 】

このセレクタの出力データは、電子透かし情報として情報信号にスクランブル情報 “ S c r a m b l e (R A M) ” を重畳する W M 書換部 2 0 6 を介して記録制御部 2 0 8 に供給される。セレクタ 2 0 5 の出力データは、W M デコード部 2 0 7 にも供給され、電子透かし情報として情報信号に重畳されているスクランブル情報の抽出、判別が行われ、判別出力がコントロール部 2 0 9 に供給される。

【 0 0 2 8 】

コントロール部 2 0 9 は入力情報から検出されたコピー制御情報および電子透かし情報の判別出力に基づいて、入力情報の記録（複製）が可能であるか否かの判別を行い、記録（複製）可能であると判別した場合は、さらに、複製制御のために電子透かし情報の書換が必要であるか否かを判別する。そして、コントロー

ル部 2 0 9 は、記録禁止と判別したときには、記録制御部 2 0 8 を制御して、記録を実行しないように制御する。また、記録可能、あるいは、1 回複製可能と判別したときには、コントロール部 2 0 9 は記録制御部 2 0 8 を制御して、記録を実行するようにし、1 回複製可能な情報信号は、スクランブル部 2 1 0 により、特定のスクランブルを施し、書き込み部 2 1 1 を介して、RAM ディスク 2 1 2 に記録するようにする。また、同時に、記録される情報信号がスクランブルされていることを示すスクランブル情報 “S c r a m b l e d (R A M) ” を WM 書換部 2 0 6 にて電子透かし情報として情報信号に重畳する。

【 0 0 2 9 】

次に、この記録再生装置での暗号解読ができた後の処理の流れを図 3 のフローチャートを参照して説明する。

【 0 0 3 0 】

まず、ステップ S 1 0 1 で、入力時に検出したコピー制御情報をチェックする。そして、次のステップ S 1 0 2 で、コピー制御情報が“絶対複製禁止”または、“これ以上複製禁止”であったかどうかを判別する。そうであった場合には、ステップ S 1 0 3 に進み、記録を禁止し、記録処理を中止する。そうでなかったとき（“複製可能”または“1 回複製可能”）には、ステップ S 1 0 4 に進む。

【 0 0 3 1 】

ステップ S 1 0 4 では、入力信号に重畳されている電子透かし情報（WM）の判定出力をチェックする。S 1 0 5 では電子透かし情報（WM）が“S c r a m b l e d”の状態であるかどうかを判別する。もしもその状態であれば、記録しようとしている情報信号は元々スクランブルされていた情報であり、これが、コピー制御情報を不正に改竄して入力された情報であると判断し、S 1 0 3 に進み、記録処理を中止する。もしもその状態でなければ、記録可能な情報であると判断する。

【 0 0 3 2 】

ステップ S 1 0 6 では、スクランブルが必要であるか否かを判断するために、“1 回複製可能”の状態にある情報信号か否かを判別する。“1 回複製可能”の状態にある場合は、ステップ S 1 0 7 で電子透かし情報を“S c r a m b l e (

RAM)”状態に書き換え、ステップS108にて、特定のスクランブル方式に従ったスクランブル処理を実施する。このようにして生成された情報をステップS109にてRAMディスクに記録する。

【0033】

“1回複製可能”に無い場合（“複製可能”の場合）は、スクランブル処理を行わずステップS109にてRAMディスクに記録する。

【0034】

以上のようなコンプライアントな記録装置によって記録されたRAMディスクは、複製制御が必要な“1回複製可能”な情報信号に対して、電子透かし情報としてのスクランブル情報と情報信号に対するスクランブルが対となって記録される。

【0035】

さらに、図2に示したように読み出し部213により読み出した信号をもとに、ディスク種別判別部214は、装填されたディスクが、ROMディスク（再生専用）であるか、RAMディスク（書込可能）であるか、さらには、1回書き込みのみ可能なディスクであるか、1000回程度書き込み可能なディスクか、10万回程度書き込み可能なディスクであるかを、物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域などから判別し、電子透かし情報にディスク種別を記録してもよい。

【0036】

なお、スクランブル処理に関しては、情報再生時の負荷を考慮し、一部の情報のみ（MPEG圧縮データのIフレームデータなど）をスクランブル対象としてもよい。この場合、電子透かし情報は、すべての情報に重畳するものとする。

【0037】

なお、上記のような情報信号をスクランブルしたROMディスクを制作するような場合には、例えば、情報記録装置がオーサリングシステムとディスクカッティングシステムとして構成され、オーサリングシステムでは、情報信号に応じて情報信号の圧縮処理を行うとともに、電子透かし情報としてスクランブル情報を重畳し、ディスクカッティングシステムでは情報信号に応じて、スクランブル処

理を施して、ディスク原盤を作成する。これを用いて、上記のような複製制御が可能なROMディスクを制作する。

【 0 0 3 8 】

〔再生装置〕

次に、実施の形態 1 のコンプライアントな再生装置について図 4 を用いて説明する。図 4 は、コンプライアントな再生装置の全体構成を示すブロック図である。この再生装置に装填されたディスクに記録されている情報は、読み出し部 4 0 1 で読み出され、デスクランブル部 4 0 2、スクランブル有無検出部 4 0 3、ディスク種別判別部 4 0 4 に供給される。

【 0 0 3 9 】

スクランブル有無検出部 4 0 3 は、付加情報としてディスクに記録されているスクランブルフラグを抽出して、記録情報にスクランブルがかかっているか否かを検出し、その検出結果をコントロール部 4 0 5 に出力する。なお、複製禁止のROMディスクには、特定暗号方式（例えば、CSS: Contents Scramble System方式など）の暗号がかけられているものとする。

【 0 0 4 0 】

ディスク種別判別部 4 0 4 は、装填されたディスクが、ROMディスク（再生専用）であるか、RAMディスク（書込可能）であるか、さらには、1 回書き込みのみ可能なディスクであるか、1 0 0 0 回程度書き込み可能なディスクか、1 0 万回程度書き込み可能なディスクであるかを、物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域などから判別し、その判別結果をコントロール部 4 0 5 に供給する。

【 0 0 4 1 】

デスクランブル部 4 0 2 は、製造元で施されたスクランブル（ROMディスクの場合）や記録装置のスクランブル部で施されたスクランブル（RAMディスクの場合）の解読を行う。

【 0 0 4 2 】

デスクランブル部 4 0 2 からの出力データは、WMデコード部 4 0 6 に供給されるとともに、再生制御部 4 0 7 に供給される。WMデコード部 4 0 6 では、電

子透かし情報として情報信号に重畳されているスクランブル情報の抽出、判別が行われ、判別出力がコントロール部 4 0 5 に供給される。

【 0 0 4 3 】

コントロール部 4 0 5 は、これらのディスク種別の判別結果、スクランブルフラグ、および電子透かし情報の判別出力に基づいて、再生を許可するか、禁止するかを決定する。コンプライアントな記録装置で記録されたディスクでは、複製制御が必要な情報信号に対し、電子透かし情報としてのスクランブル情報と情報信号に対するスクランブルが対となっている。

【 0 0 4 4 】

このため、これに違反するようなディスクが装填された場合には、その制御情報を再生制御部 4 0 7 に供給して、この再生制御部以降の処理を禁止する。正規のディスクの場合には、再生制御部以降の処理が有効となり、ビデオデータのデコーダ部 4 0 8 に供給されて、MPEG 圧縮されていたデータが伸長復号される。そして、伸長復号されたデータは、アナログ I/F 4 0 9 において D/A 変換され、外部の機器に供給される。また、デジタル I/F 4 1 1 に接続される機器がある場合には暗号化部 4 1 0 で MPEG 圧縮されたデータを暗号化し、デジタル I/F 4 1 1 から送出する。

【 0 0 4 5 】

次に図 5 を用いて参照して、この実施形態のコンプライアントな再生装置の処理動作について説明する。

【 0 0 4 6 】

再生装置では、まず、ステップ S 2 0 1 において、装填されたディスクに記録されている情報信号に、スクランブルがかかっているか否かを判別する。スクランブルには、記録装置のスクランブル部でかけられる RAM ディスク用のスクランブル方式のものと、CSS 方式等の ROM ディスク用のスクランブルがあり、これらを識別するためにステップ S 2 0 2 において、ディスク種別をチェックする。

【 0 0 4 7 】

ROM ディスクである場合、ステップ S 2 0 3 にて ROM 用のデスクランブル

処理を行う。ステップ S 2 0 4 ではスクランブルされていたかどうかを示す電子透かし情報 (WM) をデスクランブルされた情報信号から検出する。そして、S 2 0 5 では電子透かし情報が “S c r a m b l e d (ROM)” の状態であるかどうかを判別し、その状態であるときには、再生を許可 (ステップ S 2 1 1) し、その状態にない時には再生を禁止 (ステップ S 2 1 2) する。

【 0 0 4 8 】

RAMディスクである場合も同様に、ステップ S 2 0 6 にてRAM用のデスクランブル処理を行う。ステップ S 2 0 7 ではスクランブルされていたかどうかを示す電子透かし情報 (WM) をデスクランブルされた情報信号から検出する。そして、S 2 0 8 では電子透かし情報が “S c r a m b l e d (RAM)” の状態であるかどうかを判別し、その状態であるときには、再生を許可 (ステップ S 2 1 1) し、その状態にない時には再生を禁止 (ステップ S 2 1 2) する。

【 0 0 4 9 】

また、ステップ S 2 0 1 でスクランブルがかかっていないと判断された場合に、デスクランブル処理を施さず情報信号の再生を行うが、ステップ S 2 0 9 にて電子透かし情報 (WM) を検出する。そして、S 2 1 0 で電子透かし情報が “S c r a m b l e d” の状態であるかどうかを判別し、その状態にあるときは、再生を禁止 (ステップ S 2 1 2) する。その状態でないとき (電子透かし情報が検出されない場合や検出された電子透かし情報が “N o n - S c r a m b l e d”) は、再生を許可 (ステップ S 2 1 1) する。

【 0 0 5 0 】

すなわち、コンプライアントな記録装置で記録されたディスクであれば、電子透かし情報WMは、“S c r a m b l e d” と記録されたものには、情報信号にもスクランブル処理が行われているはずである。それにもかかわらず、電子透かし情報WMに “S c r a m b l e d” と記録されている情報信号がスクランブルされていない場合は、コンプライアントな再生装置の出力をディスクに記録した場合や、情報信号に施されているスクランブルを不正にデスクランブルし、ディスクに記録するなどの不正な複製が行われたことを意味しており、上記のような記録装置ならびに再生装置を用いればこのような場合の再生を禁止することが可

能である。

【0051】

これにより、再生装置にWM書換手段を実装しなくとも、不正な複製の防止が可能であり、再生装置のコストダウンが容易となる。

【0052】

なお、一部の情報信号のみがスクランブルされているような場合には、情報信号のスクランブルフラグのみではなく、デスクランブル処理が実際に行われたかどうかをデスクランブル部でチェックすることが必要である。これにより、不正に複製した情報信号のスクランブルフラグをスクランブル状態に書き換えるといった不正に対しても、再生を禁止することが可能となる。ここでは、スクランブルにより情報信号に対する暗号化を行ったが、他の方式を用いて暗号化を行った場合も同様の効果を得ることができる。

【0053】

なお、実施の形態1では、光ディスクを情報記録媒体として用いた場合について説明したが、他の半導体メモリや磁気記録媒体（ハードディスクなど）についても同様である。

【0054】

（実施の形態2）

実施の形態1では、記録装置ならびに再生装置においてディスクからの情報信号の再生や、ディスクへの情報信号の記録を行うブロックと電子透かし情報の検出や情報信号の圧縮／伸長するブロックとが一体となっている場合について説明した。PCで記録装置や再生装置を実現する場合、ドライブ部とエンコーダ／デコーダ部とを別にした構成が一般的である。

【0055】

別構成とした場合、ドライブで検出したディスク種別をもとにデコーダ部で再生制御を行うため、ディスク種別の不正なすり替えが発生すると、不正に複製したディスクが再生可能となってしまう。例えば、ROMディスクに記録された情報信号をノンコンプライアントな記録装置によりRAMディスクに記録され、再生する時には、ドライブ部とデコーダ部の間で不正なソフトウェアが介在するこ

とで、ドライブの検出したディスク種別を“ROM”とすりかえることが可能である。この結果、ROMディスクをすべてRAMディスクへ不正複製した場合にコンプライアントな再生装置で再生を防止できなくなる。実施の形態2は、このような課題を解決するための構成について説明する。

【0056】

〔PCによる記録装置〕

コンプライアントな記録装置をパーソナルコンピュータ（PC）システムで実現する構成例について図6を用いて説明する。

【0057】

図6に示すように、このコンプライアントなPCによる記録装置は、図2のコンプライアントな記録装置の構成例において入力端子からスクランブル部までをPCエンコーダ、書き込み部をPC記録ドライブとして分離し、その間を不正な複製を防止可能なデジタルI/F（SCSIやATAPI，IEEE1394など）で接続し構成される。

【0058】

PCエンコーダでは、コンプライアントな記録装置の構成例（図2）において入力端子からスクランブル部までの動作は同様であり、動作の異なる点について説明する。

【0059】

1回複製可能な情報信号は、スクランブル部610により特定のスクランブルを施す。この際、スクランブルの基となる鍵情報をPC記録ドライブとPCエンコーダ間で安全に共有するために、認証部613とPC記録ドライブ中の認証部617との間でお互いが正規のライセンスを受けた装置であるか否かを確認するために、デジタルI/F615，616を介して相互認証を行う。認証が成立した場合は、さらにデジタルI/F上に伝送するデータを暗号化するためのバス鍵を共有する。このようにして、共有化されたバス鍵を用いて、PCエンコーダでは、暗号化部614において保護が必要なデータ（鍵情報や情報信号など）を暗号化し、デジタルI/F615を介してPC記録ドライブに送信する。

【0060】

PC記録ドライブでは、共有化したバス鍵をもとに受信したデータを暗号解読部618で復号する。送信された情報信号は、書き込み部611によって、RAMディスクに記録する。鍵情報など特定の保護領域に記録する必要があるデータに関しては、PCエンコーダに対する認証が成立していない限り、書き込まないように記録制御部619にて、記録制御を行う。

【0061】

この際、ディスク種別や記録されている情報信号によって、相互認証の方式や鍵情報と情報信号に対する処理方法に違いがあるため、読み出し部620の再生信号をもとに物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域などから判別をディスク種別判別部621で行い、コントロール部622に出力する。コントロール部622では、ディスク種別にあわせて認証方式、データの伝送方式などを切り替え、PCエンコーダとのデータ伝送を行う。

【0062】

次に、このPCの記録装置での処理の流れを図7および図8の処理フローを参照して説明する。図7はPCエンコーダのコントロール部609の処理フローであり、図8はPC記録ドライブのコントロール部622の処理フローである。

【0063】

1回複製可能な情報信号を記録する場合、情報信号の記録に先立って正規にライセンスを受けた機器であるか否かを確認するため、ステップS301、S401にて相互に認証を行う。ステップS302、S402では双方がコンプライアントな装置であるか否かを判別する。認証が成立した場合は、ステップS303、S403にて共通なバス鍵を生成する。次に、S304、S404において、スクランブルに用いる鍵情報をこの共有したバス鍵をもとに暗号化あるいは改竄防止処理を施して、PC記録ドライブからPCエンコーダに転送を行う。

【0064】

PCエンコーダのコントロール部609では、図3と同様に示した記録フローにしたがって、情報信号の記録を行う。図3との相違点は、ステップS106の“1回複製可能”の判別後に、相互認証が成立しているか否かのチェックを行う

ステップ S 3 1 1 が挿入されていることであり、相互認証が成立していない場合は、記録禁止とする。

【 0 0 6 5 】

PC 記録ドライブのコントロール部 6 2 2 では、認証が成立している場合は、ステップ S 4 0 5 にて、スクランブルされた情報信号、ならびにスクランブル鍵情報やスクランブル制御情報等へのアクセス（記録や再生）が許可され、また、認証が不成立の場合は、ステップ S 4 0 6 にて、情報信号のみの記録を許可する。

【 0 0 6 6 】

したがって、コンプライアントな機器同士でないと、スクランブル鍵情報やスクランブル制御情報等へのアクセスが防止可能となる。この結果、複製制御が必要な 1 回複製可能な情報信号の記録において、コンプライアントな PC システム（エンコーダと記録ドライブの組合せ）では、電子透かし情報「スクランブル」と情報信号に対するスクランブルとが行われることとなり、ノンコンプライアントな PC システムでは、ディスク上の特定領域へのアクセスができず、正しいスクランブルの実施を防止できる。

【 0 0 6 7 】

〔 PC による再生装置 〕

次に、コンプライアントな再生装置をパーソナルコンピュータ（PC）システムで実現する構成例について図 9 を用いて説明する。図 9 に示すように、このコンプライアントな PC による再生装置は、図 4 のコンプライアントな再生装置の構成例においてデスクランブル部から出力部までを PC デコーダ、読み出し部を PC 再生ドライブとして分離し、その間を不正な複製を防止可能なデジタル I/F（SCSI や ATAPI, IEEE 1394 など）で接続し構成される。

【 0 0 6 8 】

この再生ドライブに装填されたディスクに記録されている情報は、読み出し部 9 0 1 で読み出され、スクランブル有無検出部 9 0 4、ディスク種別判別部 9 0 3 に供給され、コンプライアントな再生装置の場合と同様にスクランブルフラグ、ディスク種別を得る。

【 0 0 6 9 】

PC再生ドライブでは、スクランブルが施されている情報信号をデジタルI/Fから出力する場合、PCデコーダとの相互認証が必要となる。認証が成立していない場合には、再生制御部913にてPC再生ドライブからの読み出しを禁止する。スクランブルが施された情報信号（複製禁止）は、PCデコーダ中のデスクランブル部902により特定のデスクランブル処理を施す。

【 0 0 7 0 】

この際、デスクランブルの基となる鍵情報をPC再生ドライブとPCデコーダ間で安全に共有するために、PC再生ドライブ中の認証部915とPCデコーダ中の認証部919との間でお互いが正規のライセンスを受けた装置であるか否かを確認するために、デジタルI/F916、917を介して相互認証を行う。正常に認証ができた場合は、さらにデジタルI/F上に伝送するデータを暗号化するためのバス鍵を共有する。このようにして、共有化されたバス鍵を用いて、PC再生ドライブでは、暗号化部914において保護が必要なデータ（鍵情報や情報信号など）を暗号化し、デジタルI/F916を介してPCデコーダに送信する。

【 0 0 7 1 】

この際、ディスク種別や記録されている情報信号によって、相互認証の方式や鍵情報と情報信号に対する処理方法に違いがあるため、読み出し部901の再生信号をもとに物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域などから判別をディスク種別判別部903で行い、コントロール部912に出力する。

【 0 0 7 2 】

コントロール部912では、ディスク種別にあわせて認証方式、データの伝送方式などを切り替え、PCデコーダとのデータ伝送を行う。PCデコーダでも同様に、再生する情報信号が記録されたディスク種別や情報信号のスクランブル方式に合わせて認証方式、データの伝送方式などを切り替る。

【 0 0 7 3 】

PCデコーダでは、共有化したバス鍵をもとに受信したデータを暗号解読部9

18で復号を行う。デスクランブル部902以降の処理は、図4で示したコンプライアントな再生装置の場合と同様である。

【0074】

コントロール部905は、情報信号のスクランブル（スクランブルの有無やスクランブル方式）や電子透かし情報のスクランブル情報による再生制御のみではなく、認証方式やデータ伝送方式なども用いて再生制御を行う。

【0075】

次に、このPCの再生装置での処理の流れを図10および図11の処理フローを参照して説明する。図10はPC再生ドライブのコントロール部912の処理フローであり、図11はPCデコーダのコントロール部905の処理フローである。

【0076】

ディスク上にスクランブルされて記録されている情報信号を再生する場合、情報信号の再生に先立って正規にライセンスを受けた機器であるか否かを確認するため、ステップS501、S601にて相互に認証を行う。ステップS502、S602では双方がコンプライアントな装置であるか否かを判別する。認証が成立した場合は、ステップS503、S603にて共通なバス鍵を生成する。次に、S504、S604において、スクランブルに用いる鍵情報をこの共有したバス鍵をもとに暗号化あるいは改竄防止処理を施して、PC再生ドライブからPCデコーダに転送を行う。

【0077】

PC再生ドライブのコントロール部906では、認証が成立している場合は、ステップS505にて、スクランブルされた情報信号、ならびにスクランブル鍵情報やスクランブル制御情報等への再生が許可され、また、認証が不成立の場合は、ステップS506にて、情報信号のみの再生を許可する。

【0078】

PCデコーダのコントロール部912では、図5と同様に示した再生フローにしたがって、情報信号の記録を行う。図5との相違点は、ステップS202のディスク種別の判別後に、ステップS609、S612にて、それぞれのディスク

に対応した相互認証が成立しているか否かのチェックを行うように変更されていることであり、相互認証が成立していない場合は、このような情報信号の再生禁止とする。

【0079】

したがって、コンプライアントな機器同士でないと、スクランブル鍵情報やスクランブル制御情報等へのアクセスが防止可能となる。この結果、複製制御が必要な複製不可能な情報信号の再生において、コンプライアントなPCシステム（デコーダと再生ドライブの組合せ）では、情報信号に対するデスクランブルと電子透かし情報「スクランブル」の検出されることとなり、ノンコンプライアントなPCシステムではディスク上の特定領域からの鍵情報の再生ができず、正規のデスクランブルを防止できる。

【0080】

次に、ディスク種別を改竄されることなくドライブ部からエンコーダやデコーダに転送する方法について詳細に図12を用いて説明する。

【0081】

〔ディスク種別転送方式〕

PCエンコーダ部やデコーダ部では、情報信号を記録再生する条件として、ディスク種別を利用している。このため、ドライブ部からエンコーダ部やデコーダ部に改ざんされることなくディスク種別を転送することが必要である。

【0082】

図12のディスクには、ドライブ部とエンコーダ/デコーダ間の相互認証に使用する認証鍵情報1201が記録されている。認証鍵情報は、相互認証に使用する共通鍵（認証鍵）と認証鍵情報が記録されるディスクの種別が個々の装置に割り当てられたデバイス鍵で暗号化された暗号化認証鍵（EAK1、EAK2、・・・）である。

【0083】

$EAK1 = ENC(\text{デバイス鍵}(DK1), \{\text{認証鍵}(AK), \text{ディスク種別}(DT)\})$

$EAK2 = ENC(\text{デバイス鍵}(DK2), \{\text{認証鍵}(AK), \text{ディスク種別}$

(DT)}}

PCドライブでは読み出した認証鍵情報から機器に割り当てられた暗号化認証鍵(EAK1)を取り出し、機器が保有しているデバイス鍵DK1で復号する。この結果、認証鍵と(AK)ディスク種別(DT)が得られる。ドライブでは、装填されたディスクに対して、物理特性(フォーカス特性、トラッキング特性、再生特性)やディスク種別を記録したコントロール領域などからディスク種別(DT')を判別する。相互認証には、認証鍵(AK)とディスク種別判別部1202からのディスク種別(DT')とを特定の演算(図中では加算)によって得られたディスク認証鍵(DAK')を用いる。

【0084】

一方、PCエンコーダ/デコーダでは、ドライブから読み出した認証鍵情報から機器に割り当てられた暗号化認証鍵(EAK2)を取り出し、機器が保有しているデバイス鍵DK2で復号する。この結果、認証鍵と(AK)ディスク種別(DT)が得られる。相互認証には、認証鍵(AK)とディスク種別(DT)とを特定の演算(図中では加算)によって得られたディスク認証鍵(DAK)を用いる。

【0085】

このようにして共有化したディスク認証鍵を用いて、相互認証を行うと $DAK = DAK'$ の場合は相互認証が成立するが、 $DAK \neq DAK'$ の場合は相互認証が成立しない。つまり認証鍵情報のDTとドライブが検出したDT'が一致しない時には、認証を不成立にすることが可能である。この結果、ディスク上にROMディスクから入手した情報信号や鍵情報をRAMディスクに不正に複製したとしても、認証鍵情報中のディスク種別(DT)とドライブが検出するディスク種別(DT')が不一致となり、相互認証が不成立となり、情報信号の再生を防止できる。また、認証鍵情報を不正にすりかえたとしても、認証鍵やディスク種別が不一致となり、相互認証が不成立となる。

【0086】

なお、認証鍵情報に認証鍵とディスク種別を暗号化して記録した場合について説明したが、認証鍵情報にディスク種別を含めずにドライブで検出したディスク

種別を暗号化してPCエンコーダやデコーダに伝送し、復号してディスク種別を得る方法でも、ディスク種別を安全に転送することができ、実質的に正常な情報信号の再生は可能である。相互認証は成立しているため、情報信号が誤ったディスク種別（スクランブル方式）で再生される場合があるため、映像や音声が正しく表示されなくなる。

【 0 0 8 7 】

上記のような記録装置ならびに再生装置によると、PCドライブ部にWM検出部やWM書換部を実装しなくても、不正な複製ディスクの再生を防止できる。

【 0 0 8 8 】

また、ディスク種別によって認証方式やデータの伝送方式（データや鍵情報の伝送手順）がことなると説明したが、この性質を逆に利用し、認証を行った処理手順から、ディスク種別の判別を行うことも可能である。ここでは、スクランブルにより情報信号に対する暗号化を行ったが、他の方式を用いて暗号化を行った場合も同様の効果が得ることができる。

【 0 0 8 9 】

なお、実施の形態2では、光ディスクを情報記録媒体として用いた場合について説明したが、他の半導体メモリや磁気記録媒体（ハードディスクなど）についても同様である。

【 0 0 9 0 】

【発明の効果】

以上説明したように、この発明によれば、これ以上複製禁止、あるいは、絶対複製禁止の情報信号に対しては、当該情報信号がスクランブルされていることを示すスクランブル情報を電子透かし情報として重畳するとともに、情報記録媒体の種別にしたがったスクランブルを行って情報記録媒体への記録を行うようにしたので、スクランブルを解読して不正に情報記録媒体へ記録したり、他の種類の情報記録媒体へ不正に複製したりしたとしても、情報再生装置にて、読み出した情報信号に重畳されている電子透かし情報としてのスクランブル情報と読み出した情報信号のスクランブルの状態をチェックすることにより、不正な複製によって作成された情報記録媒体からの再生を防止することができる。なお、本発明に

よれば、情報再生装置にて、電子透かし情報の書換は行わないので、電子透かし情報の書換手段を実装する必要が無く、安価な構成をとることが可能である。

【図面の簡単な説明】

【図 1】

複製世代管理方法の実施の形態 1 の概略図

【図 2】

実施の形態 1 の情報信号記録装置の概略構成図

【図 3】

実施の形態 1 の情報信号記録装置の制御フローチャート

【図 4】

実施の形態 1 の情報信号再生装置の概略構成図

【図 5】

実施の形態 1 の情報信号再生装置の制御フローチャート

【図 6】

実施の形態 2 の情報信号記録装置の概略構成図

【図 7】

実施の形態 2 の P C エンコーダの制御フローチャート

【図 8】

実施の形態 2 の P C 記録ドライブの制御フローチャート

【図 9】

実施の形態 2 の情報信号再生装置の概略構成図

【図 1 0】

実施の形態 2 の P C 再生ドライブの制御フローチャート

【図 1 1】

実施の形態 2 の P C デコーダの制御フローチャート

【図 1 2】

実施の形態 2 の認証方式を示す図

【図 1 3】

従来の複製世代管理方法を示す図

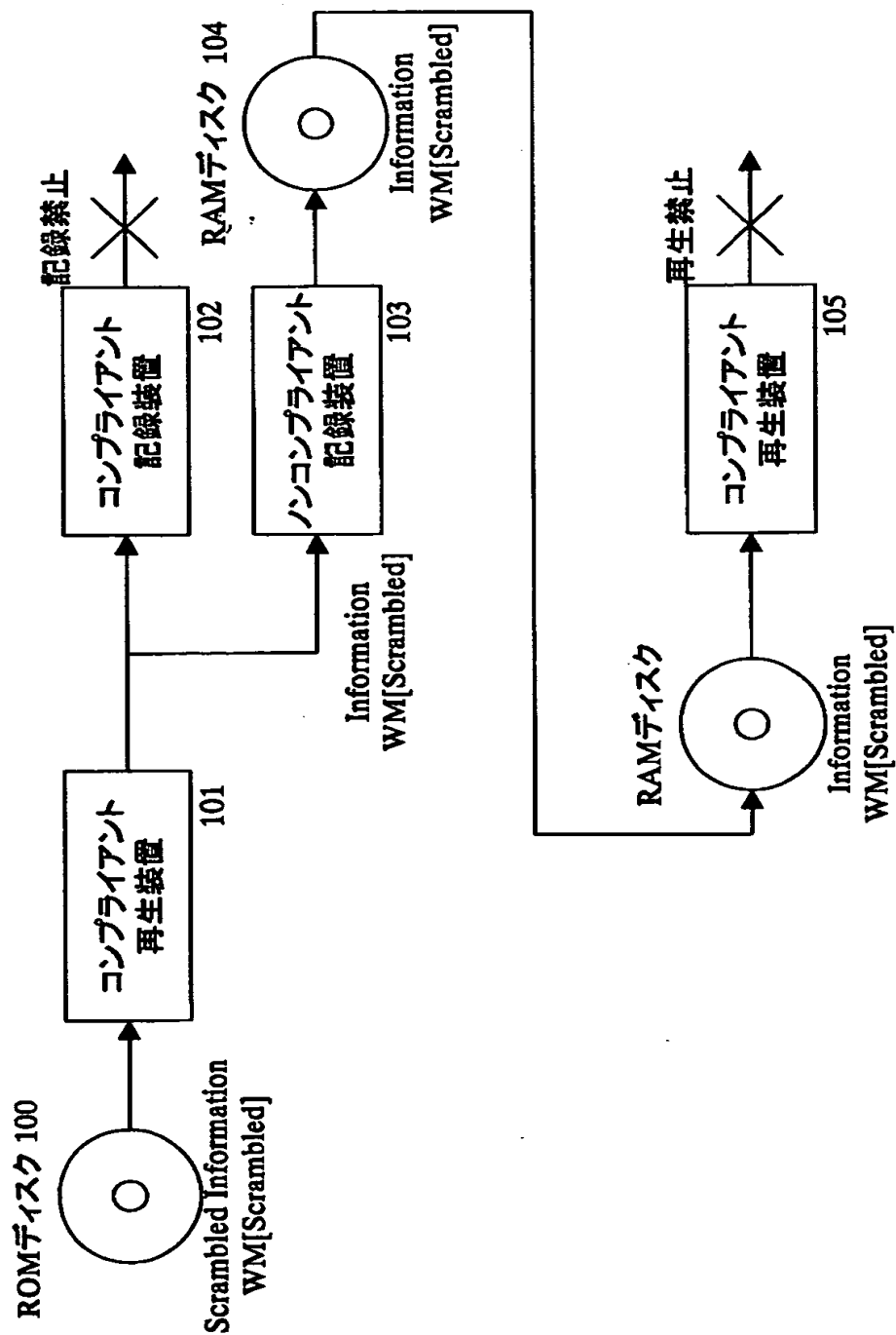
【符号の説明】

- 1 0 1 コンプライアントな再生装置
- 1 0 2 コンプライアントな記録装置
- 1 0 5 コンプライアントな再生装置
- 2 0 1 デジタル I / F
- 2 0 2 アナログ I / F
- 2 0 3 暗号解読部
- 2 0 4 エンコード部
- 2 0 6 WM書換部
- 2 0 7 WMデコード部
- 2 0 8 記録制御部
- 2 0 9 コントロール部
- 2 1 0 スクランブル部
- 2 1 1 書込み部
- 2 1 3 読み出し部
- 2 1 4 ディスク種別判別部
- 4 0 1 読み出し部
- 4 0 2 デスクランブル部
- 4 0 3 スクランブル有無検出部
- 4 0 4 ディスク種別判別部
- 4 0 5 コントロール部
- 4 0 6 WMデコード部
- 4 0 7 再生制御部
- 4 0 8 デコード部
- 4 0 9 アナログ I / F
- 4 1 0 暗号化部
- 4 1 1 デジタル I / F

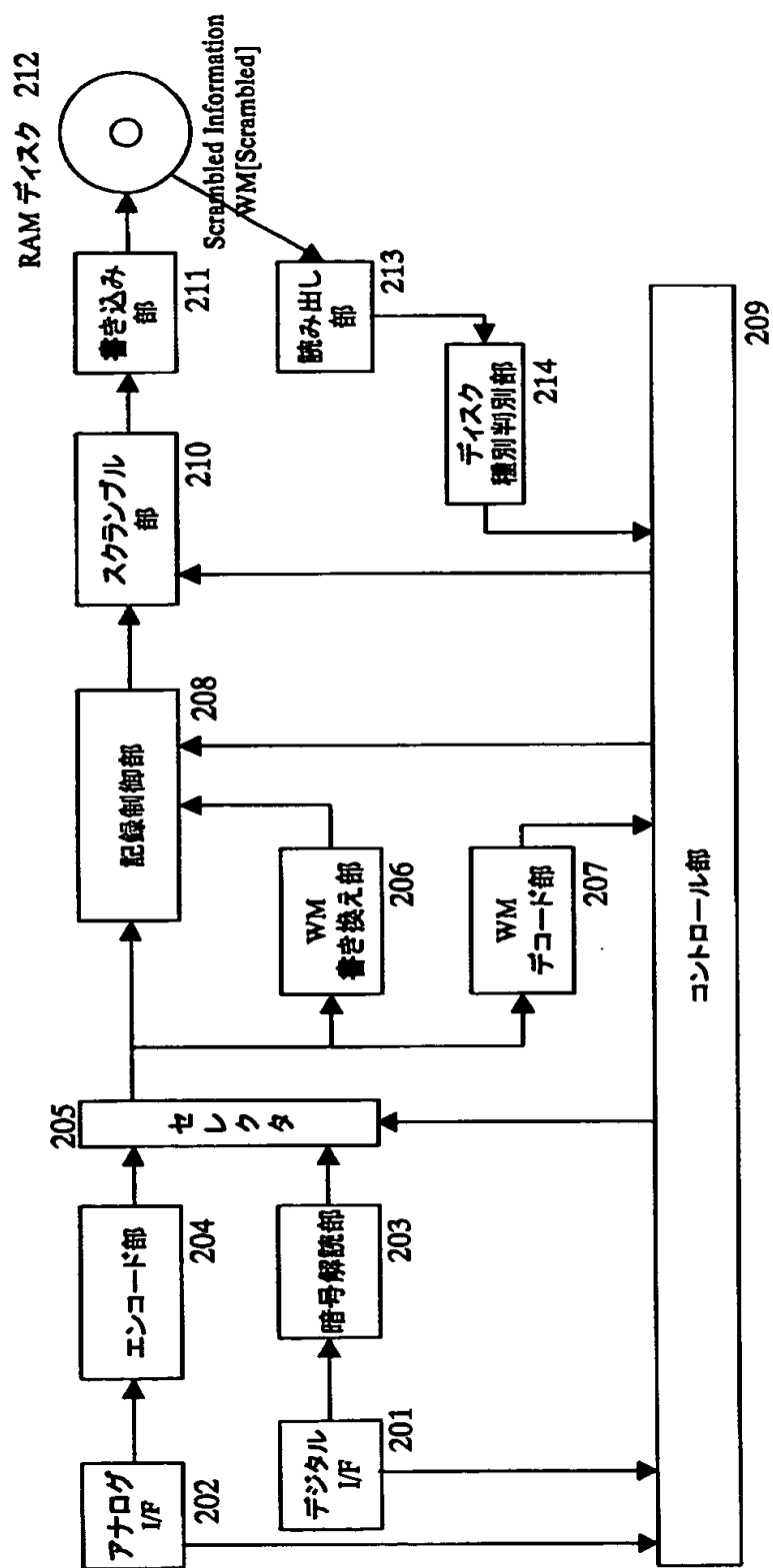
【書類名】

図面

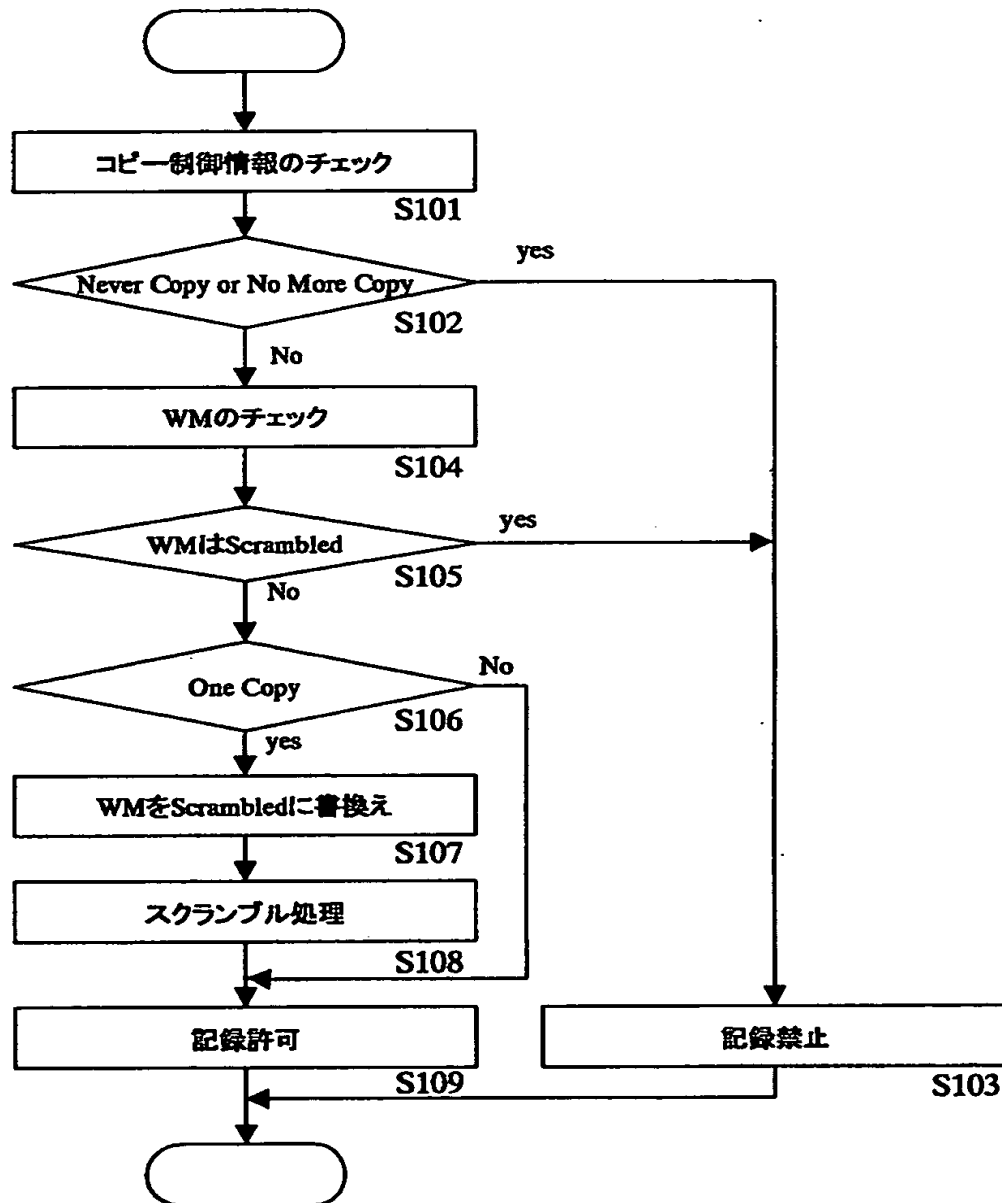
【図 1】



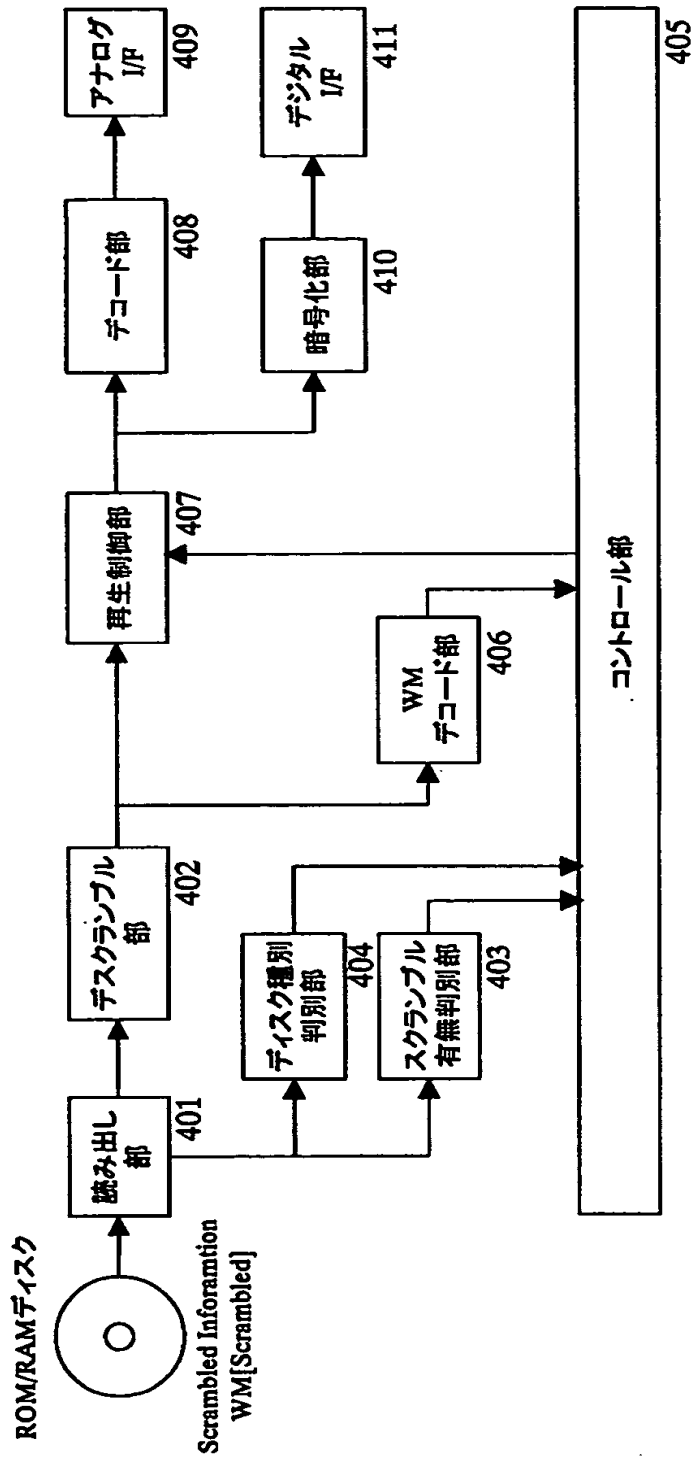
【図 2】



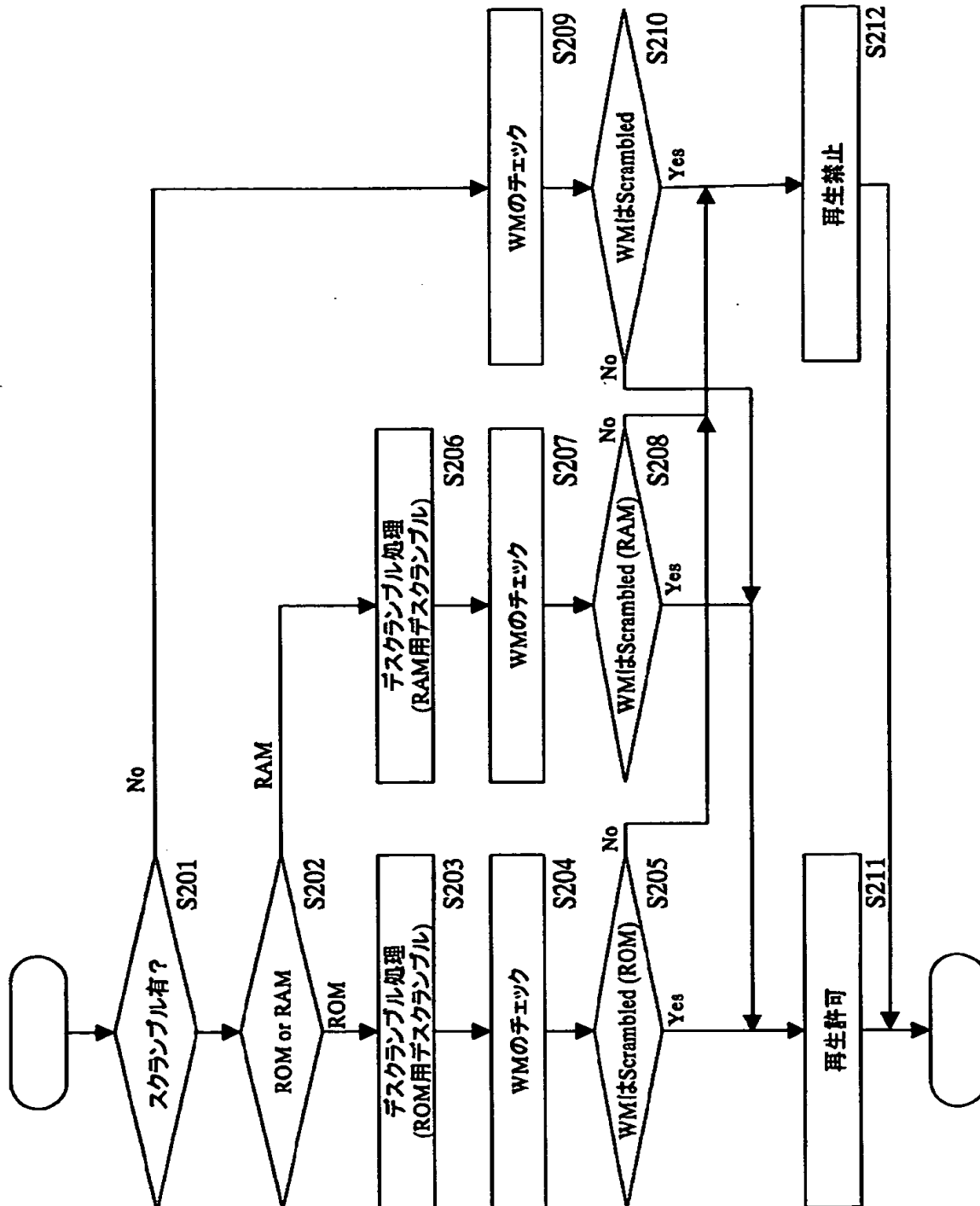
【図 3】



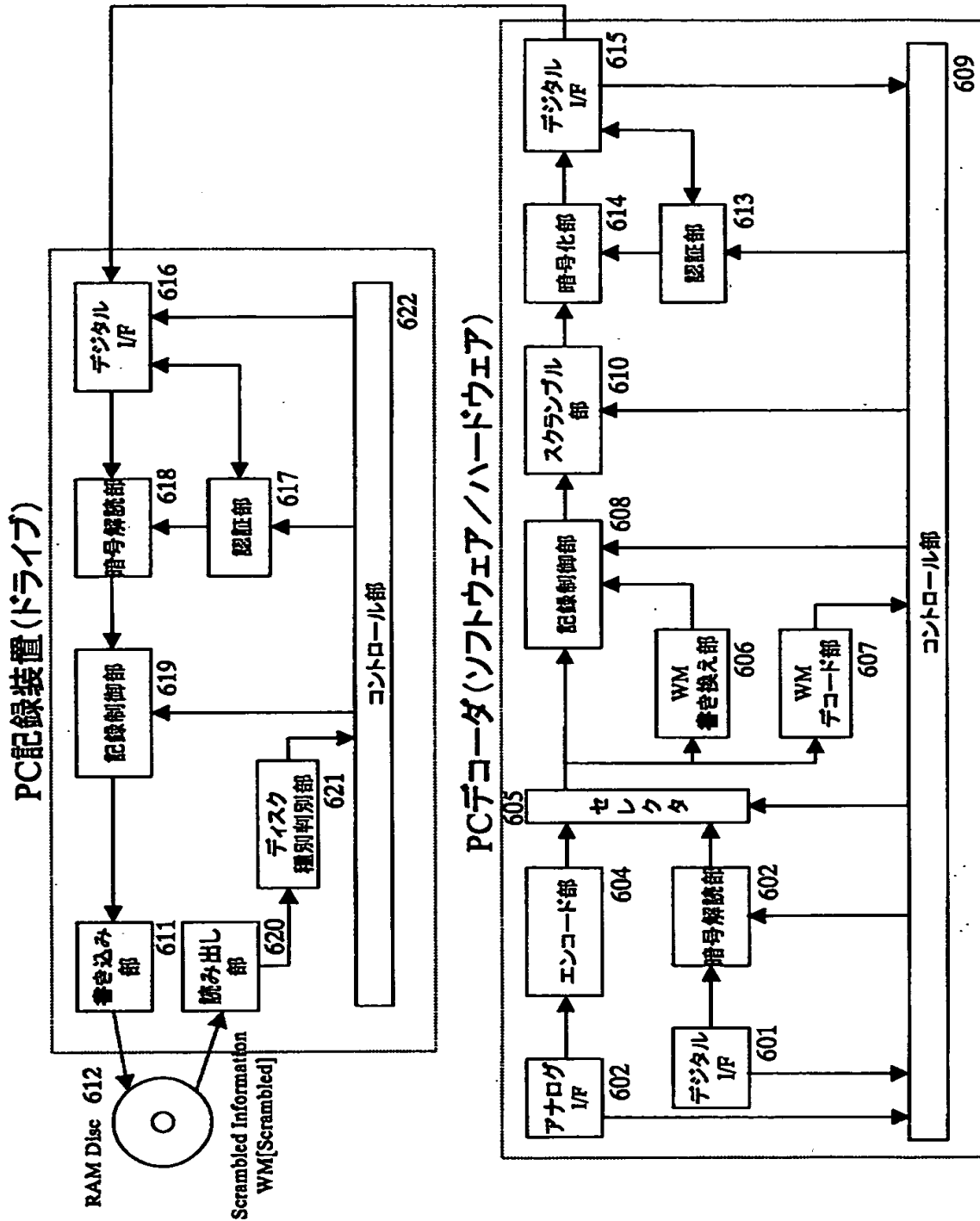
【図 4】



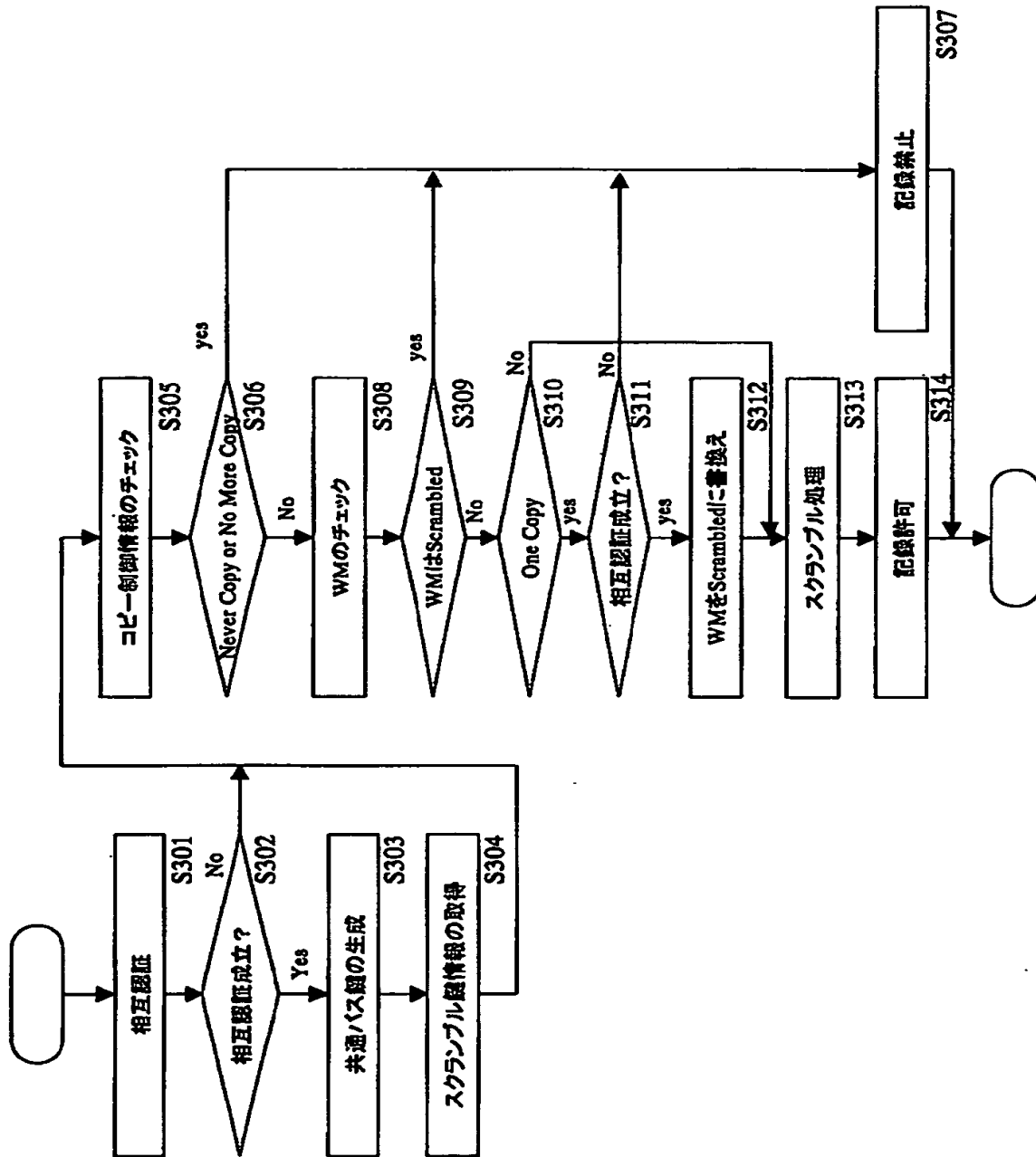
【图 5】



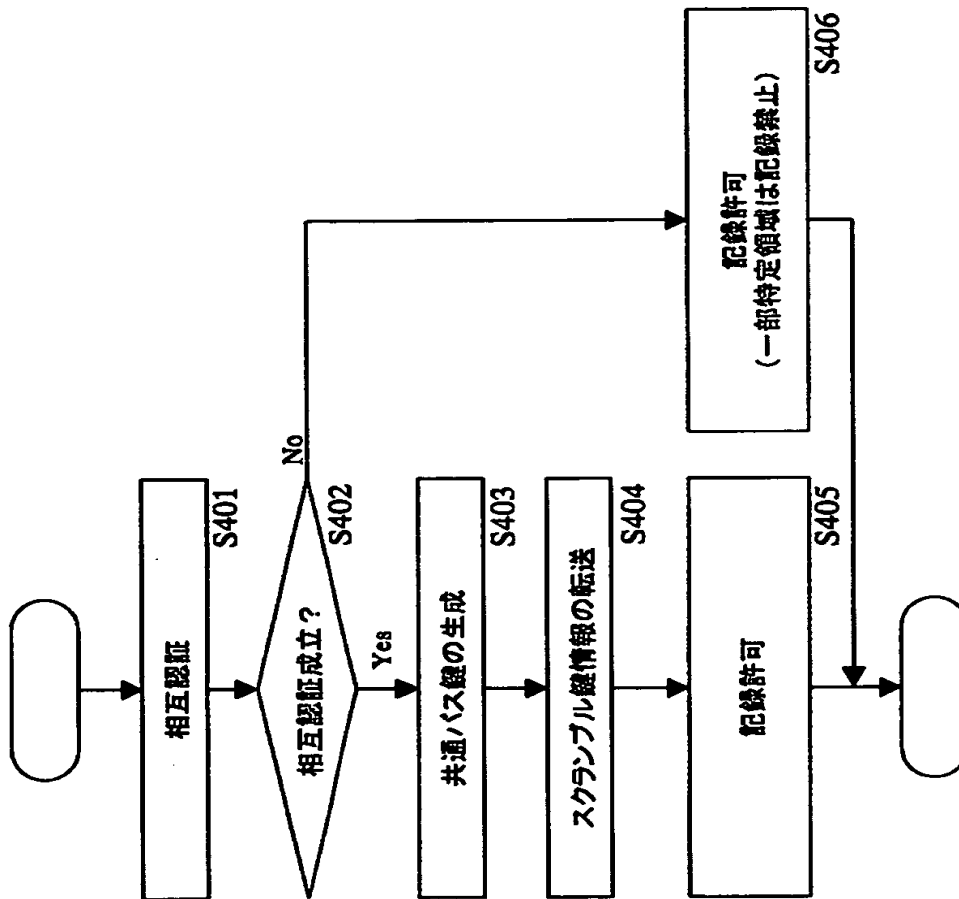
【図 6】



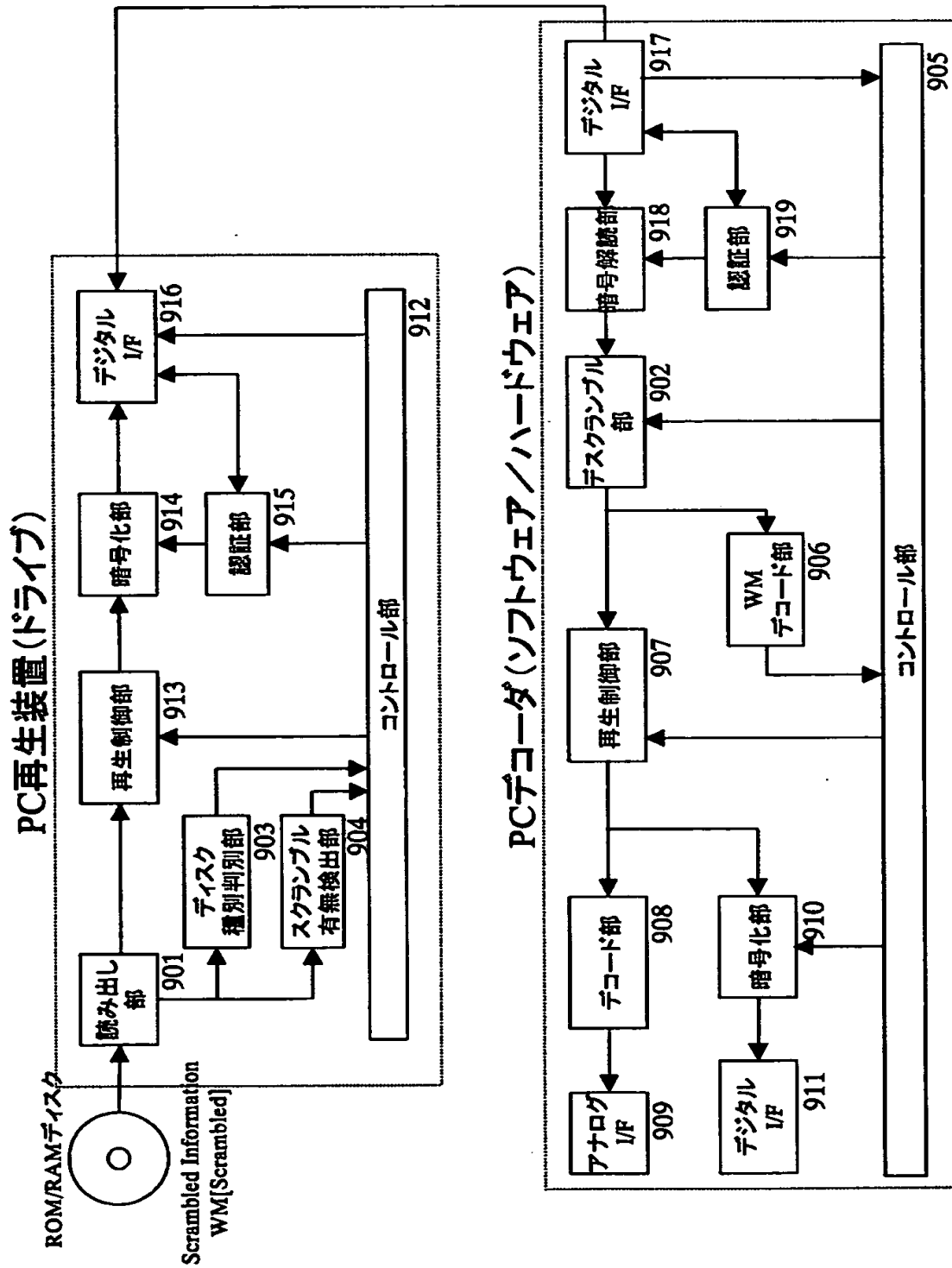
【図 7】



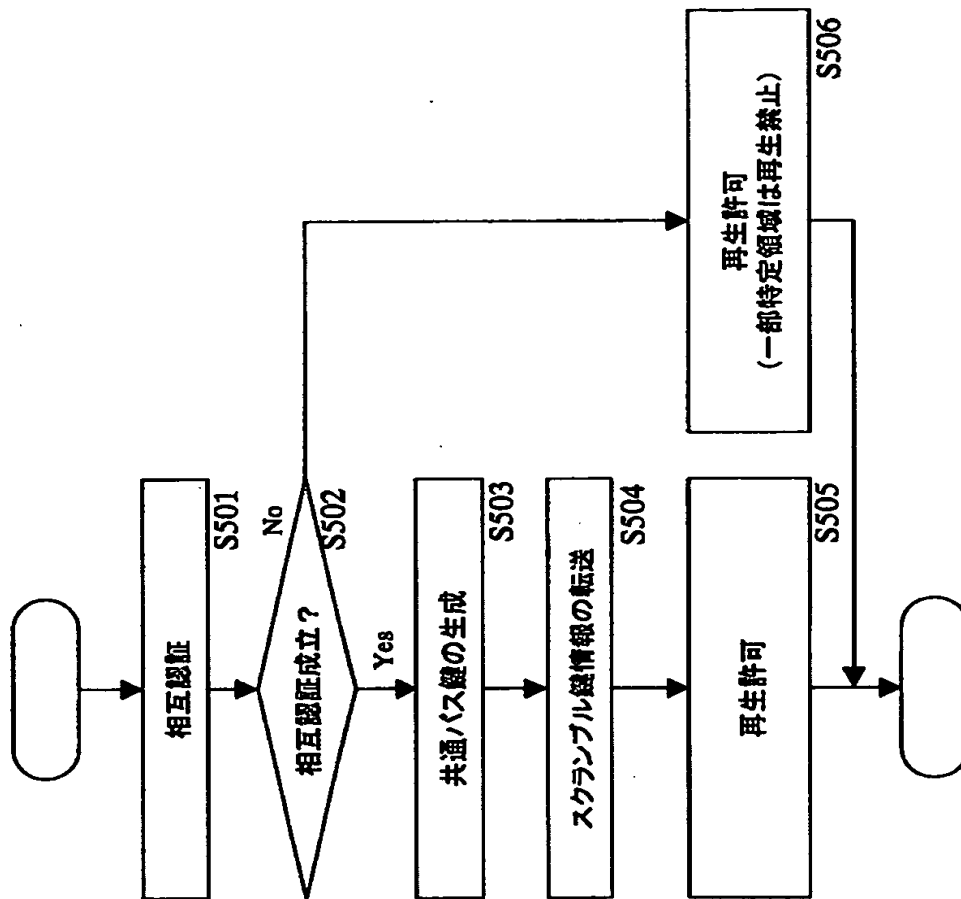
【図 8】



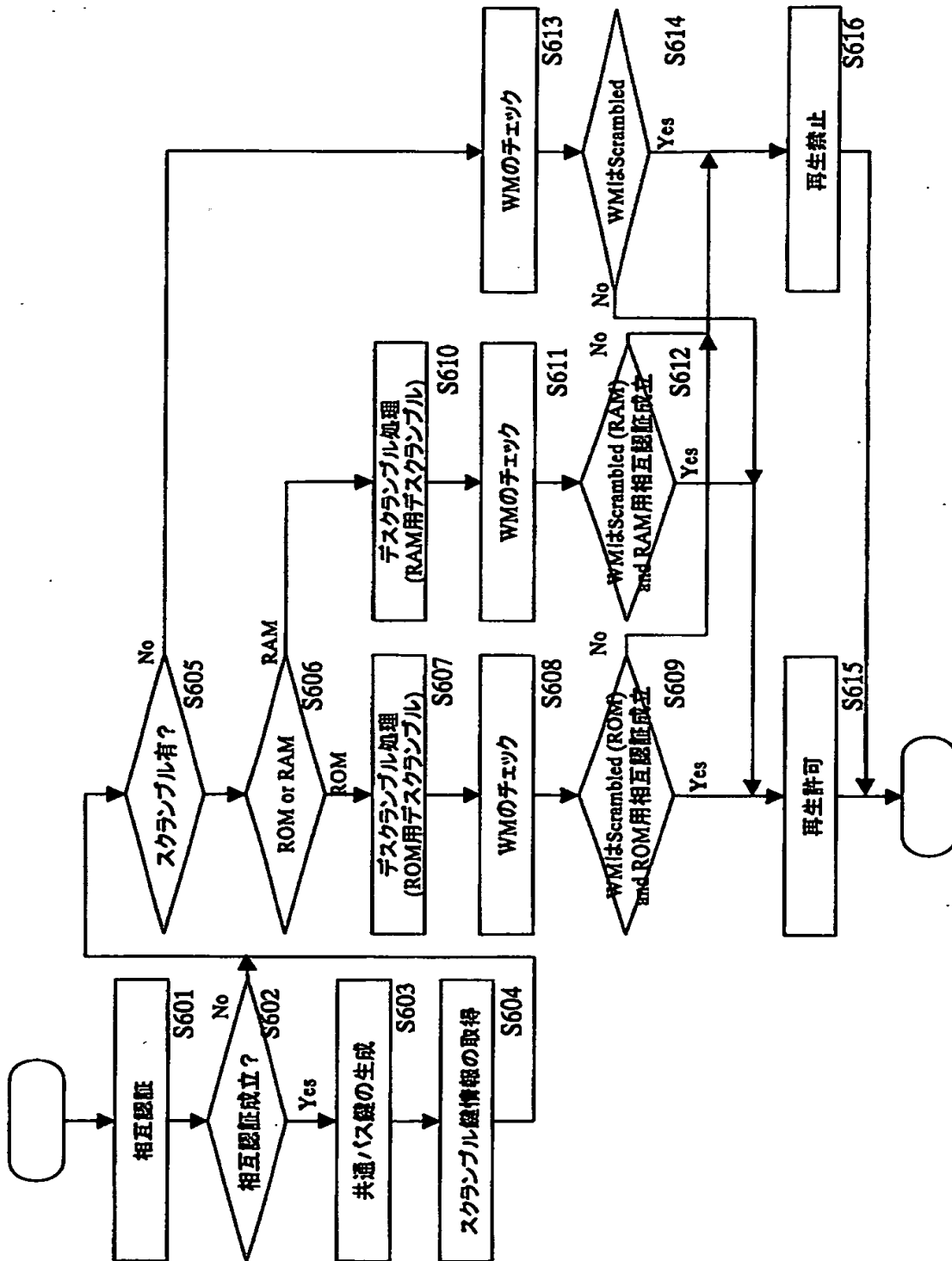
【图9】



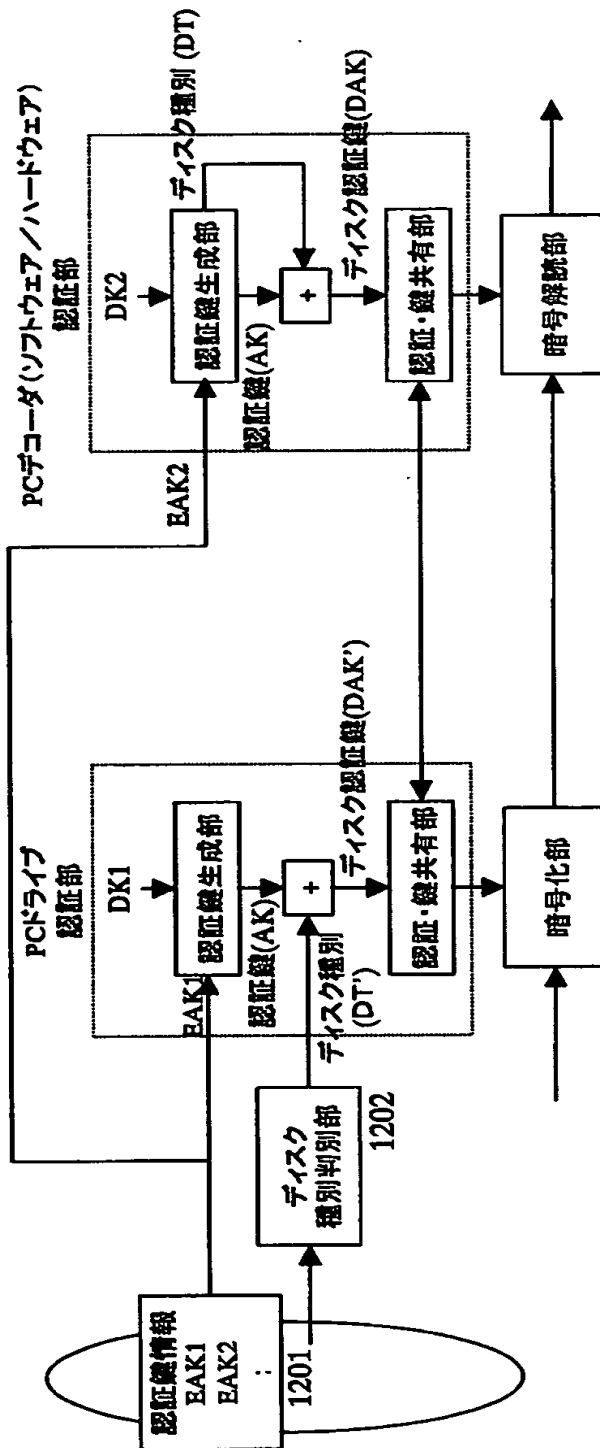
【図 1 0】



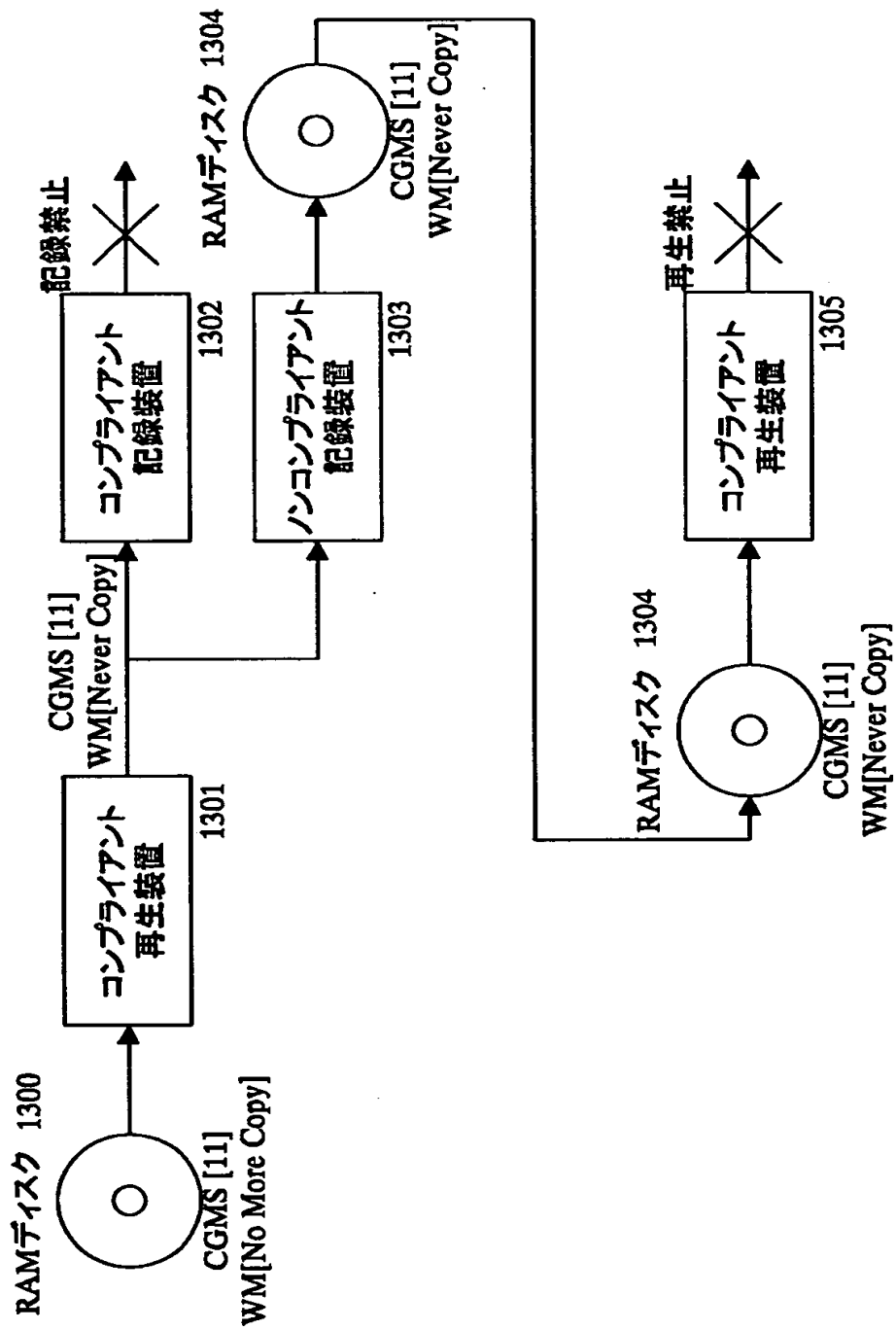
【図 11】



【図 12】



【図 1 3】



【書類名】 要約書

【要約】

【課題】 違法に作成された記録媒体からの情報信号の再生を実質的に不能にすることにより、有効で安価な複製の防止ができる方法および装置を提供する。

【解決手段】 複製制御のために、少なくとも、“1回複製可能”、“これ以上の複製禁止”、“絶対複製禁止”の3状態を有する複製制御情報を前記情報信号に付加して伝送する複製世代管理方法であって、“これ以上の複製禁止”、あるいは“絶対複製禁止”の状態に有る情報信号にスクランブル情報を示す電子透かし情報を重畳し、さらに、前記情報信号にスクランブルを行い、情報記録媒体に記録する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社